CONTINUATION OF APPLICATION FOR A SEARCH WARRANT

INTRODUCTION

1. I, Aaron Eastham, am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed since 2018. I am currently assigned to the Detroit Field Office, Grand Rapids Resident Agency. During my employment with the FBI, I have conducted investigations involving violations of federal criminal laws, including violations related to child exploitation and pornography. I am familiar with the various statutes of Title 18, United States Code, Chapter 110 – sexual exploitation and other abuse of children, including violations pertaining to sexual exploitation and attempted sexual exploitation of children (18 U.S.C. § 2251(a)), distribution or receipt of child pornography (18 U.S.C.§ 2252A(a)(2)) and possession of child pornography (18 U.S.C. § 2252A(a)(5)(B)), the "subject offenses." I am a federal law enforcement officer and, therefore, authorized by the Attorney General to request a Search Warrant under Federal Rule of Criminal Procedure 41.

2. I make this Continuation in support of an Application for a Search Warrant for the residence of **1675 W 32nd St, Holland, MI 49423** (hereinafter the "SUBJECT PREMISES"), to search for evidence of sexual exploitation and attempted sexual exploitation of children, distribution or receipt of child pornography, and possession of child pornography, and to search the person of Todd ACHTERHOF for evidence of the same. Child pornography is any visual depiction of a minor depicting the lascivious exhibition of the genitals or sexually explicit conduct, *see* 18 U.S.C. § 2256(8).

3. The statements contained in this Continuation are based on information acquired during my investigation, as well as information provided by others such as other police officers, and task force officers (TFOs) and special agents of the FBI. Because this Continuation is being submitted for the limited purpose of establishing probable cause to secure a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe necessary to establish probable cause to believe that there is evidence of criminal activity in violation of 18 U.S.C. §§ 2251(a)), 2252A(a)(2), and 2252A(a)(5)(B) at the SUBJECT PREMISES (further described in Attachment A).

PROBABLE CAUSE FOR SEARCH WARRANT

4. Between May 25, 2023 and April 20, 2024, an FBI Under Cover (UC) made several post on a forum dedicated to incest called "Ins-Dream Forum" alluding to having an incestuous relationship with his daughter. On January 18, 2024, the UC made a post including his Session ID.

5. Starting around March 29, 2024, a Session user named "Tastytreat" (later identified as TODD ACHTERHOF) messaged the UC on Session and said he was from the ins dream forum and was a fellow dad. He then said he had a 12-year-old daughter that he was teaching to be careful, which took some time. He then said he started doing sexual things with her about a year prior, when she was 11, which included oral sex and fingering/jacking off.

6. ACHTERHOF described his first experience with her when his daughter was in his lap and he felt her chest and felt guilty. He then said now he

cuddles with her and it leads to more but he no longer feels guilty. He then said he had "rubbed myself on her a lot, but never entered." He said because she has not had her period yet, he would like to "finish deep inside her" but "part of me worries about the consequences."

7. After the UC said he had been with his daughter once in the shower, ACHTERHOF said "I'm definitely going to try the shower idea now."

8. ACHTERHOF said he "played" with his daughter 3 or 4 times a month when her mom is gone.

9. ACHTERHOF told the UC that he lived in Northern Vermont.

10. ACHTERHOF told the UC that he hadn't filmed or taken pictures of the things he has done with his daughter. He said "I worry about showing faces or distinguishing background features. That said, I love to have pictures or a short video of her in my phone."

11. On April 1, 2024, ACHTERHOF sent the UC a photo of a blue pair of male underwear next to a pink pair of underwear, on a bathmat next to the shower. He told the UC that he had showered with his daughter and they performed oral sex on each other. He claimed his daughter wanted to have sex and he thought it might happen tonight or tomorrow. The UC asked several times for photos to see what ACHTERHOF's daughter looked like, but did not receive any. He said he struggled with posting pictures and wanted to keep chatting.

12. ACHTERHOF sent an image of a pair of underwear that he claimed were his daughter's. On April 4, 2024 he sent a photo of what appeared to be a

laundry basket with several pairs of children's underwear in it.

13. On April 05, 2024, he sent a photo of what appeared to be a child's buttocks, in jeans, through the opening in the back of a folding chair. On April 11, 2024, ACHTERHOF send another photo of a buttocks wearing black leggings.

14. He described his daughter has petite, with brown hair and brown eyes. In the chats he called her Ellie.

15. The UC asked ACHTERHOF if he had Kik. ACHTERHOF said that he didn't but would download it. He asked about if Kik needed a phone number or e-mail to register, and the UC told him that he could just use a fake e-mail. ACHTERHOF expressed concern over Kik's privacy policy. On April 12, 2024, the UC gave ACHTERHOF his Kik username and ACHTERHOF said he would add him the next day.

16. On April 13, 2024, ACHTERHOF messaged the UC on Kik (username tastytreats4). He sent the UC the two images of the buttocks he had sent previously on Session. He claimed the picture of the buttocks in the black yoga pants was his daughter Ellie.

17. ACHTERHOF sent several photos of a child, however none of the photos including the face of the child. In one photo a girl was laying on a bed in black shorts and a t-shirt. A hand is touching the child's leg. Another image was a close up photo of a buttocks in jeans. Another phot depicted a hand on the bare legs that appear to be the size of a child's legs.

18. ACHTERHOF claimed that his daughter wanted him to have sex with

her and that she told him this. On April 18, 2024, he described the previous night with his daughter. His story included his daughter initiating them showering together, before going to her room and performing oral sex on each other before he fingered her and attempting to have penile intercourse with her. He claimed his daughter asked him to ejaculate on her vagina.

19. On April 23, 2024, ACHTERHOF said that his daughter told her friend that she "messed around with a guy," which made him nervous and that he was going to back off Kik as a precaution, and wished the UC luck with his daughter.

20. On April 28, 2024, ACHTERHOF sent the UC a video depicting a girl, who appeared to be under the age of 18, masturbating with a dildo. A banner across the screen said "I can't moan my dad is home". He sent some photos of girls in bathing suits, and said he got them from a group on Telegram.

21. ACHTERHOF then said that his daughter promised not to tell anyone about what they do together. He then began talking about his daughter's friend "Sarah" and that her breasts were more developed than his daughters.

22. ACHTERHOF said he talked to his daughter about taking pictures and videos and said she was okay with it and they agreed not to show faces or identifying stuff.

23. On May 02, 2024, ACHTERHOF sent a photo he claimed was his daughter of the close-up crotch area of a female in grey underwear. On May 11, 2024, he sent a photo depicting a close up photo of a vagina that he cropped, but claimed was of his daughter.

24. On April 29, 2024, an administrative subpoena was served to Kik for the account associated with the username "tastytreats4". On May 1, 2024, Kik responded to the subpoena and provided various IP addresses for the account. A birthday of XX/XX/1974 was listed for the account user.[1] The registration date of the account was 04/13/2024.

25. Activity from the IP address 47.46.54.30 was the most used IP in the return and was utilized 202 times by the user between 4/14/2024 and 4/30/2024. The IP address belonged to Charter Communications.

26. On May 10, 2024, an administrative subpoena was served to Charter Communications. On May 16, 2024, Charter responded to the subpoena, however, due to issues with the Charter Online Portal, the return was not accessed until May 20, 2024. Charter Communications responded with the following subscriber information:

a. Todd Douglas Achterhof

b. Address: 1675 W 32nd St, Holland, MI, 49423-4368

27. Open-source database checks identified ACHTERHOF as:

a. Todd Douglas Achterhof

b. DOB:XX/XX/1974 (Age 49)[2]

---

[1] Kik provided the full date of birth for the account user. It is known to me, and I can disclose the information to a judicial officer upon request. However, I have omitted the precise date from this continuation since it is a publicly filed document.

[2] As before, the full date of birth for ACHERHOF is known to me, but I have removed the complete information to keep it off the public record. However, the date of birth provided for ACHTERHOF by Charter Communications matches the date of

c. SSN: XXX-XX-9476[3]

28. A review of ACHTERHOF's public facing social media accounts revealed that he had a 15-year-old son, a 13-year-old son, a 10-year-old daughter, and a 7-year-old-son. He also worked as a Captain at Graafschap Fire Department and was a Campus Safety Dispatcher at Hope College.

CHARACTERISTICS COMMON TO INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

29. Based upon my knowledge, experience, and training in child exploitation and CP investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals with a sexual interest in children. These characteristics particularly apply to individuals involved in possessing or distributing CP online, including those accessing websites whose primary content is CP. These common characteristics include that the individuals:

a. Generally have a sexual interest in children and receive sexual gratification from viewing children engaged in sexual activity or in sexually suggestive poses, or from literature describing such activity.

b. May collect or view sexually explicit or suggestive materials, in a

---

birth provided by Kik concerning the user of the Kik account that was chatting with the UC.

[3] The complete social security number is known to me and can be disclosed to a judicial officer upon request. However, I have removed the complete social security from this document in order to keep such information from appearing in a publicly filed document.

variety of media, including in hard copy and/or digital formats. CP viewers and collectors oftentimes use these materials for their own sexual arousal and gratification. They may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse or groom a child to participate in sexual activity, or to demonstrate desired sexual acts to a child. They may also use toys, games, costumes, sexual clothing, sexual paraphernalia, and children's clothing to lure or entice children. They may keep "trophies" or mementos of sexual encounters with children, or items that they use to gratify a sexual interest in children, such as by collecting children's underwear or other items belonging to a child.

c. May take photographs that either constitute CP or indicate a sexual interest in children by using cameras, video cameras, web cameras, and cellular telephones. Such images and videos may be taken with or without the child's knowledge. This type of material may be used by the person to gratify a sexual interest in children.

d. Generally maintain their collections in a safe, secure, and private environment. These images and videos can be downloaded onto desktop or laptop computers, computer disks, disk drives, data disks, system disk operating systems, magnetic media floppy disks, Internet-capable devices, cellular telephones, tablets, digital music players, and a variety of electronic data storage devices (hardware, software, diskettes, tapes, CDs, DVDs, SD cards, memory cards, USB/jump/flash memory devices, external hard drives, and other digital storage media). The images can be stored in both digital and hard copy format and are usually hidden so that

they are not found by other members of the residence or by anyone else who enters the home. Such hiding places could include but are not limited to garages, sheds, attics, vehicles, bags, and pockets. Digital files and devices may be password protected, encrypted, or otherwise protected.

e. Often maintain their collections of CP and other materials indicating a sexual interest in children for a long period of time—commonly over the course of several years. These collections are also frequently maintained despite changes in residence or the acquisition of different or newer computer devices.

f. May correspond with and/or meet others to share information and materials; rarely destroy correspondence from other CP distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, screen names, and telephone numbers of individuals with whom they have been in contact and who share the same interests in CP. Such correspondence may take place, for example, through online bulletin boards and forums, Internet-based chat messaging, email, text message, video streaming, letters, telephone, and in person. In some cases, these individuals may have joint involvement in CP activities with others within their household or with whom they share a close relationship (e.g., brothers/siblings dating partners, or coworkers).

SPECIFICS OF SEIZING AND SEARCHING COMPUTER SYSTEMS

30. Computers and Internet-capable devices such as tablets and cellular

telephones facilitate access to CP. The Internet affords collectors and viewers of CP several different venues for obtaining, viewing, and trading CP in a relatively secure and anonymous fashion.

31. Storage capacity of computers and portable storage media, such as USB or thumb drives, has grown tremendously within the last several years. These drives can store thousands of images at very high resolution, are easily transportable, and are relatively inexpensive. Advances in technology have significantly reduced the size of digital storage devices such that now large numbers of digital files can be stored on media that will fit in a person's pocket, on a keychain, or in any number of easily transportable and concealable places. An individual can now easily carry on his or her person storage media that contains thousands of files, including images, video files, and full-length movie files.

32. As with most digital technology, communications made from a computer device are often saved or stored on that device. Storing this information can be intentional, for example, by saving an email as a file on the computer or saving the location as a "favorite" website in a "bookmarked" file. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be stored automatically in many places, such as temporary files or Internet Service Provider (ISP) client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files.

33. A forensic examiner often can recover evidence that shows whether a

computer device contains peer-to-peer software, when the device was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten.

34. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

35. Searches and seizures of evidence from computers and computer devices commonly require agents to download or copy information from the

computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

g. Computer storage devices can store the equivalent of millions of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

h. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

36. In order to retrieve data fully from a computer system, the analyst needs all storage devices as well as the central processing unit (CPU). In cases involving CP where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

37. To examine the computer and digital media properly, it may also be necessary to seize certain other items including documentation of programs, passwords, notes, or even specialized hardware. Therefore, this warrant seeks permission to seize not only the digital storage media and to search it for evidence in the form of CP images or videos, stored emails associated with the receipt and distribution of such images, and any chat or other text files relating to contact with collectors of CP or with actual children, but also requests permission to seize all hardware, software, and computer security devices necessary to access and examine the computer storage media. Peripheral equipment including printers, routers, modems, network equipment used to connect to the Internet may also contain evidence of what devices were used to connect to the Internet, who used those devices, and what actions the person(s) performed while using such devices.

38. Forensic examiners can also find the presence or absence of certain software and programs to determine who controlled a computer at a given time.

Such evidence includes: viruses, Trojan horses, spyware, malware, and other forms of malicious software; the presence or absence of security software designed to detect malicious software; the lack of malicious software; and the presence or absence of software designed to protect a device from infiltration, access, or control by another person or entity, which may include pop-up blockers, security software, password protection, and encryption. Forensic examiners can also find evidence of software or programs designed to hide or destroy evidence.

39. The time period required for a complete, safe, and secure forensic examination of the computer and storage media is uncertain. The government will make available for pick-up within a reasonable time all items found not to contain any contraband or material to be seized pursuant to the warrant and all hardware and software no longer needed for examination purposes. In conducting the search, the forensic examiner and agents will examine files regardless of their name because such names and file extensions can be altered to conceal their actual content. Because of the volume of data to be searched and the need to complete the examination in a reasonable time, the forensic examiner will also use computer techniques such as keyword searches that may result in the display of irrelevant materials.

40. Attempts will be made to preview items on-scene, in order to exclude items unlikely to contain evidence or individuals with no involvement in the subject offenses. Items determined on-scene not to contain items listed in Attachment B will be left at the SUBJECT PREMISES. The remaining items will be seized and

searched for further review or forensic examination and will be returned as soon as reasonably possible if they are determined not to contain evidence listed in Attachment B.

41. Retention of any computers would be warranted, if any CP is found thereon, in order to permit forfeiture of those computers and related properties as instrumentalities of the crime, pursuant to 18 U.S.C. §§ 2253(a)(3) and 2254(a)(2).

42. I am aware that the recovery of data by a computer forensic analyst takes significant time. For this reason, the Return inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the Return will not include evidence later examined by a forensic analyst.

AFTER HOURS SEARCH REQUEST

43. I received the above information identifying ACHTERHOF as the target of this investigation on today's date, 5/20/2024. As discussed above, ACHTERHOF has boasted of having repeated sexual access to his daughter and described an escalating series of sexual assaults that also include the likely production of child pornography. I have also verified that ACHTERHOF has a 10-year-old daughter, meaning that there could be an imminent risk of further sexual assaults committed by ACHTERHOF against his child. For these reasons, I submit there is good cause to execute this search warrant at any time day or night.

CONCLUSION

44. Based upon the above information, I respectfully submit there is

probable cause to believe that on the person of Todd ACHTERHOF and within the SUBJECT PREMISES there will be evidence of sexual exploitation and attempted sexual exploitation of children (18 U.S.C. § 2251(a)), distribution or receipt of child pornography (18 U.S.C.§ 2252A(a)(2)) and possession of child pornography (18 U.S.C. § 2252A(a)(5)(B)), the "subject offenses."

45. Wherefore, by this Continuation and Application, I respectfully request that the Court issue a Search Warrant authorizing the search of the person of Todd ACHTERHOF and the SUBJECT PREMISES, described in Attachment A for items listed in Attachment B, and the seizure of those items for the purpose of searching and analyzing them off-site.